TO: National Security Council
FROM: Ghost in the Shellcode [W. DeSombre, M. Lee, E. Plankey, B. Saunders]
RE: Downstream Effects from Cyber Attack on Qatari Water Treatment Facility

---

EXECUTIVE SUMMARY

A cyber attack on a Qatari water treatment plant led to minor disruptions and mass panic during the 2022 World Cup. A Chinese firm attributed the attack to the United States without publicly sharing evidence. The incident **risks increased short-term U.S. diplomatic tensions** with France and Qatar, as well as **long-term potential impacts on U.S. industrial control systems**. The U.S. must pursue a policy of **aid and attribution diplomacy (COA2)**. COA2 provides solutions for domestic resiliency, concrete steps to engage France and Qatar, and mitigates diplomatic spillover of allegations against the U.S.

BACKGROUND

On November 21, 2022, the Qatari Ras Abu Fontas water treatment plant suffered from a **disruptive cyberattack**, stemming from backdoored **Yuma Industrial Control Systems (ICS)** software. The disruption began on the first day of the 2022 World Cup. While the disruption lasted only eleven hours, leaked information caused panic, demand spikes, and water shortages in migrant communities.

Fenghuang Labs, a Chinese incident response firm hired by Qatari Electricity & Water Co, attributed the attack to the United States without publicly sharing any evidence. In response to Fenghuang's attribution claims, the **French National Police have privately threatened to decrease cooperation with the United States on combating cybercrime** if more evidence indicates U.S. perpetration of the attack. Independent researchers have also accused the United Arab Emirates, citing poor UAE/Qatari relations, although the UAE has denied these claims.

THREAT & RISK ASSESSMENT

Short-term Diplomatic Tensions **[Severity: High | Likelihood: High]**

- Fenghuang Labs **attributed the attack to the U.S.**, leading to diplomatic tensions with allies (France) and regional partners (UAE, Qatar). **We do not have U.S. intelligence confirming this analysis**. Tensions with France and Qatar can increase risks to the USCENTCOM airbase in Qatar and the U.S.-French partnership to combat cybercrime.

Long-term ICS Cyber Defense **[Severity: Medium | Likelihood: Medium]**

- The Yuma ICS compromise may affect all organizations using the latest version of its temperature control software. **We do not know how many U.S.-based desalination and water treatment plants use Yuma software**. If a similar incident happens on U.S. soil, mass panic would likely have more impact than the service disruption itself. Clear, transparent, and timely communication is crucial to any emergency response plan.

STRATEGIC OBJECTIVES

Any course of action must **maintain relationships with key regional partners** and allies like Qatar and France, **ensure reliability and availability of U.S. critical infrastructure**, and **ensure regional stability** within the Middle East.

COURSES OF ACTION

COA1 – BASELINE — FULL TRANSPARENCY

CISA, **USCERT,** and **WaterISAC** enumerate a list of U.S. companies running Yuma software. **FBI/NCIJTF** publicly offers to collaborate with local law enforcement in **Qatar, Morocco, and Chile** to conduct a forensic investigation of impacted systems. **State Department** issues an advisory on the World Cup, echoing the Qatari government's statement on fully functioning water reserves. **State Bureau of Cyberspace and Digital Policy** issues a statement on the importance of protecting world cultural events, including both Expo 2020 and the World Cup.

Advantages	*Disadvantages*
Showcases U.S. support for affected countries and indicates lack of involvement with the attack. Proactively addresses possible U.S. vulnerabilities.	Does not address claim of U.S. responsibility. Has limited engagement with the private sector.

COA2 – MODERATE ESCALATION — AID & ATTRIBUTION DIPLOMACY

All of COA1, and: State and **FBI** push a joint statement that **USG** is using all available sources to conduct an investigation. **U.S. Intelligence Community (IC)** conducts private attribution of the Yuma backdoor and destructive malware using all available sources and methods. **FBI** privately reaches out to **French OCLCTIC** to assist with law enforcement collaboration and engages **U.S. private sector partners** (e.g., Mandiant, Crowdstrike) to attribute malware found during the investigation. **USAID** offers to ship bottled water stockpiles to Qatari regions not connected to water reserves.

Advantages	*Disadvantages*
Reaffirms commitment to French foreign law enforcement partners to smooth Qatari-U.S. tensions.	Parallel U.S. investigation increases potential tensions with the Chinese government.

COA3 – HIGH ESCALATION — PREPARE DEFENSES

All of COA1 and COA2, and: U.S. Press Secretary gives a public denouncement of Fenghuang attribution and announces a public investigation into Fenghuang Chinese government ties. **DOD** notifies **Al Udeid Air Base** to watch for anti-U.S. retaliatory protests that may occur near the base.

Advantages	*Disadvantages*
Mitigates potential criticism of insufficient USG response should attacks continue. Ensures safety of U.S. citizens abroad in Qatar.	Risks perception of acting disproportionately. Antagonizes Qatari and Chinese diplomatic relations.

RECOMMENDATION: COA2 - Aid and Attribution Diplomacy

Short-Term Impacts: **Reaffirms** diplomatic commitment to French allies, provides immediate support to affected Qatari communities, **assures** access to actionable intelligence including malware samples and potential U.S. targets, and **mitigates** diplomatic spillover of allegations against U.S.

Long-Term Impacts: **Increases** operational readiness between USG and private sector investigatory capacity, **mitigates** future risks to U.S. targets by identifying malign actors to impose future costs.